Transport Layer Security (TLS)

Transport Layer Security (TLS), a successor to SSL, ensures the privacy of data sent between applications and Redis databases. TLS also secures connections between Redis Enterprise Software nodes.

You can use TLS authentication for the following types of communication:

- Communication from clients (applications) to your database
- Communication from your database to other clusters for replication using Replica Of
- Communication to and from your database to other clusters for synchronization using Active-Active

Protocols and ciphers

TLS protocols and ciphers define the overall suite of algorithms that clients are able to connect to the servers with.

You can change the TLS protocols and ciphers to improve the security of your Redis Enterprise cluster and databases. The default settings are in line with industry best practices, but you can customize them to match the security policy of your organization.

Client-side encryption

Client-side encryption may be used to help encrypt data through its lifecycle. This comes with some limitations. Operations that must operate on the data, such as increments, comparisons, and searches will not function properly. Client-side encryption is used to help protect data in use.

You can write client-side encryption logic directly in your own application or use functions built into clients such as the Java Lettuce cipher codec.

Updated: April 15, 2022